



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

h: A

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/712,474	11/12/2003	Duc Pham	AESN3008CON1	9332
23488	7590	11/21/2006	EXAMINER DEBNATH, SUMAN	
GERALD B ROSENBERG NEW TECH LAW 260 SHERIDAN AVENUE SUITE 208 PALO ALTO, CA 94306-2009			ART UNIT 2196	PAPER NUMBER

DATE MAILED: 11/21/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

## Office Action Summary

Application No.

10/712,474

Applicant(s)

PHAM ET AL.

Examiner

Suman Debnath

Art Unit

2196

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

### Status

- 1) ☐ Responsive to communication(s) filed on \_\_\_\_.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

### Disposition of Claims

- 4) ☒ Claim(s) 1-35 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-35 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_ are subject to restriction and/or election requirement.

### Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 11/12/03 is/are: a) ☐ accepted or b) ☒ objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

### Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
  - ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_.
  - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- \* See the attached detailed Office action for a list of the certified copies not received.

### Attachment(s)

- |  |   |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)            | 4) <input type="checkbox"/> Interview Summary (PTO-413)           |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)   | Paper No(s)/Mail Date. ____                                       |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| Paper No(s)/Mail Date <u>11/02/06</u>  | 6) <input type="checkbox"/> Other: ____                           |

### **DETAILED ACTION**

1. Claims 1-35 are pending in this application.

#### ***Drawings***

2. The drawing 12B is objected to as failing to comply with 37 CFR 1.84(p)(4) because reference character "386" has been used to designate both "REPORT POLICY FAILURE" and "CREATE LAB" in FIG. 12B. Corrected drawing sheets in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the application. Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. Each drawing sheet submitted after the filing date of an application must be labeled in the top margin as either "Replacement Sheet" or "New Sheet" pursuant to 37 CFR 1.121(d). If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

#### ***Specification***

3. The disclosure is objected to because of the following informalities:  
  
Reference character "36" is used to designate as "a file system" ([0084], line 3) and "agent program" ([0045], line 9, [0046], line 2, [0080], line 8) in specification.  
  
Reference character "52" is used to designate as "SYSTEM CONTROL HUB" in FIG. 2 but "52" is used to designate as "the chipset" ([0051], line 2) in specification.

Art Unit: 2196

Reference character "34" is used to designate as "AUTH FILE SYSTEM" in FIG. 5 but "34" is used to designate as "the modified file system" ([0045], line 1) in specification.

Reference character "180" is used to designate as "a policy parser" ([0078], line 1) and "the policy processor" ([0079], line 3) in specification.

Reference character "386" is used to designate as "failures being reported" ([0115], line 5) and "the combined data is resegmented" ([0115], line 16) in specification to describe FIG. 12B.

Appropriate correction is required.

### ***Claim Objections***

4. Claims 12 and 27 are objected to because of the following informalities:

Claim 12 recites the limitation "the generation of a modified file request" in line 2. There is insufficient antecedent basis for this limitation in the claim.

Claim 27 recites the limitation "the specification" in line 2. There is insufficient antecedent basis for this limitation in the claim.

Appropriate correction is required.

### ***Double Patenting***

5. The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory obviousness-type double patenting rejection is appropriate where the conflicting claims are not identical, but at least one examined application claim is not patentably distinct

Art Unit: 2196

from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., *In re Berg*, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent either is shown to be commonly owned with this application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement.

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

6. Claims 1-3, 5-20, 22, 24 and 30-35 are rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1-9, 12, 19, 21-23 and 26-30 of U.S. Patent No. 6,678,828 B1, hereinafter "'828 application", issued to Pham et al. Although the conflicting claims are not identical, they are not patentably distinct from each other because of the following reasons:

7. Claim 1 of the instant application corresponds to claim 1 of '828 application, specifically in that the instant application is a broader characterization of the same invention.

8. Claim 2 of the instant application corresponds to claims 2 and 4 of '828 application, as follows: **authentication data includes user and session data (instant application); authentication data defines a session with respect to the execution of said**

application program (claim 2 in '828 application); authentication data includes a verified user identifier (claim 4 in '828 application).

9. Claim 3 of the instant application corresponds to claim 12 of '828 applictaion, as follows: **authentication data includes a secure signature of said application program (instant application)**; secure data protocol provides for the digital signing of the said first file data (claim 12 in '828 application).

10. Claim 5 of the instant application corresponds to claim 12 of '828 application, as follows: **generate a secure signature of said application program and provide said secure signature as part of said authentication data (instant application)**; secure data protocol provides for the digital signing of said first file data (claim 12 in '828 application).

11. Claim 6 of the instant application corresponds to claim 8 of '828 application, specifically in that the instant application is a broader characterization of the same invention, as follows: **network appliance includes a policy parser operative to evaluate said authentication data and a policy data store including predetermined policy data accessible by said parser (instant application)**; network appliance further includes an access policy store which stores a plurality of predetermined access policies, and wherein said network appliance is operative to qualify said file data request

Art Unit: 2196

against said plurality of predetermined access policies stored by said access policy store (claim 8 in '828 application).

12. Claim 7 of the instant application corresponds to claim 9 of '828 application.

13. Claim 8 of the instant application corresponds to claims 1 and 8 of '828 application, specifically in that the instant application is a broader characterization of the same invention.

14. Claim 9 of the instant application corresponds to claim 4 of '828 application, as follows: **authentication data includes an authenticated identification of a user associated with said application program (instant application);** authentication data includes a verified user identification (claim 4 of '828 application).

15. Claims 10, 11, 12 and 14 of the instant application corresponds to claims 2, 12, 21 and 5 of '828 application, respectively.

16. Claim 13 of the instant application corresponds to claim 26 of '828 application, specifically in that the instant application is a broader characterization of the same invention.

Art Unit: 2196

17. Claim 15 of the instant application corresponds to claims 6 and 7 of '828 application, as follows: **policy data store further provides for the storage of an encryption key identifier determinable by said policy parser on evaluation of said file request message (instant application);** network appliance provides for the storage of meta-data, including an encryption key identifier, in correspondence with said predetermined network file and wherein said network appliance provides for the retrieval of said meta-data (claim 6 of '828 application); **network appliance obtains an encryption key identified by said encryption key identifier for use in the cipher processing of file data transferred in connection with said modified file request (instant application);** network appliance includes an encryption key store and wherein said encryption key identifier selects an encryption key provided to said encryption unit in connection with said second file data request (claim 7 of '828 applicaion).

18. Claims 16, 17, 18, 19, 20, 22, 24 of the instant application corresponds to claims 8, 19, 3, 4, 22, 23, 19 of '828 application, respectively. Specifically in that the instant application is a broader characterization of the same invention.

19. Claim 30 of the instant application corresponds to claims 26 and 30 of '828 application, specifically in that the instant application is a broader characterization of the same invention.



20. Claim 31 of the instant application corresponds to claims 27 and 28 of '828 application, specifically in that the instant application is a broader characterization of the same invention.

21. Claim 32, 33, 34 and 35 of the instant application corresponds to claim 29 of '828 application.

***Claim Rejections - 35 USC § 102***

22. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

23. Claims 1-35 are rejected under 35 U.S.C. 102(e) as being anticipated by Graham et al. (Pub. No.: US 2002/0178271 A1), hereinafter "Graham".

24. As to claim 1, Graham discloses a network storage architecture supporting securely controlled access and transfer of data between a client computer system and a network data store (FIG. 1, [0064]), said network storage architecture comprising: a) an agent program ([0064], lines 11-14, client module reads on agent program), operative

with respect to an application program ([0118], lines 8-12), executed on a client computer system (FIG. 1, item 150), executable by said client computer system to access a network data store ([0064], lines 1-5), to develop authentication data with respect to said application program (FIG. 4, [0128]) ; and b) a network appliance, coupleable through a communications network to said client computer system (FIG. 1, proxy system 110, [0067], lines 1-10), interoperable with said agent program to receive and validate said authentication data ([0066], line 2-11, as describes the proxy system which determines if the requesting user has the right to access the file reads on receiving and validating the authentication data), said network appliance providing a response message to said agent program to control execution of said application program ([0066], lines 7-11).

25. As to claim 2, Graham discloses that the authentication data includes user and session data ([0160], lines 1-4, lines 6-8, Graham inherently teaches of including user and session data as part of authentication data by identifying the entity with whom the server and client are communicating and by ensuring the live-ness, i.e., the current session as part of authentication service).

26. As to claim 4, Graham discloses the agent program operative to obtain user authentication and collect data with respect to user sessions and processes to develop said authentication data ([0128], line 1-4)

Art Unit: 2196

27. As to claim 5, Graham discloses that the agent program is further operative to generate a secure signature of said application program and provide said secure signature as part of said authentication data ([0216]-[0217], Graham inherently teaches of generating a secure signature by including a signature flag that indicates the payload has been signed by the source).

28. As to claim 6, Graham discloses a policy parser operative to evaluate said authentication data (FIG. 3, item 226, [0101], lines 6-12, The management service modules reads on the policy parser) and a policy data store including predetermined policy data accessible by said policy parser (FIG. 3, policy database 370, [0115], lines 1-4).

29. As to claim 7, Graham discloses that the predetermined policy data, as evaluated by said policy parser, is determinative of said response message ([0107], lines 7-11).

30. As to claim 8, Graham discloses a network storage architecture supporting securely controlled access and transfer of data between a client computer system and a network data store (FIG. 1, [0064]), said network storage architecture comprising: a) an agent program ([0064], lines 11-14, client module reads on agent program), executed on a client computer system (FIG. 1, item 150), responsive to a source file request

Art Unit: 2196

issued with respect to a network data store by an application program executed by said client computer system ([0118], lines 8-12), said agent program being operative to develop authentication data with respect to said application program ([0128], lines 1-4, authentication service module is operative as part of client module, e.g., see FIG. 4) and to provide a file request message including a representation of said source file request and said authentication data ([0065], lines 9-14); and b) a network appliance, coupleable through a communications network to said client computer system (FIG. 1, proxy system 110, [0067], lines 1-10) and responsive to said file request message ([0066], lines 7-11), said network appliance including a policy parser operative to evaluate said file request message (FIG. 3, item 226, [0101], lines 6-12, The management service modules reads on the policy parser) and a policy data store including predetermined policy data accessible by said policy parser (FIG. 3, policy database 370, [0115], lines 1-4), said network appliance, responsive to the evaluation of said file request message ([0107], lines 7-11), enabling performance of said source file request with respect to said network data store ([0106], lines 3-8).

31. As to claim 9, Graham discloses the authentication data includes an authenticated identification of a user associated with said application program ([0128], lines 1-4, FIG. 4).

32. As to claim 10, Graham discloses the authentication data includes user session and context data ([0160], lines 1-4, lines 6-8, Graham inherently teaches of including user session and context data as part of authentication data by identifying the entity with whom the server and client are communicating and by ensuring the live-ness, i.e., the current session as part of authentication service).

33. As to claims 3 and 11, Graham discloses that the authentication data includes a secure signature of said application program ([0213], lines 2-6, [0217], which describes a signature flag that indicates the payload has been signed by the source reads on including a secure signature).

34. As to claim 12, Graham discloses the network appliance that enables the generation of a modified file request corresponding to said source file request and direct to said network data store ([0106], lines 3-8, FIG. 1, Graham inherently teaches the generation of modified file request in order to pass the request from client 150 to proxy system 110 then to network storage 160 by supporting NFS protocol which is used access and modify the NAS file-system).

35. As to claim 13, Graham further discloses comprising a first communications network through which said file request message is received by said network appliance

([0067], lines 1-10) and a second communications network through which said modified file request is provided to said network data store ([0080], lines 9-14).

36. As to claim 14, Graham discloses wherein said network appliance includes an encryption unit ([0092], lines 1-3, Graham teaches of using an encryption engine within the content subsystem; [0066], lines 7-11, Graham teaches of including an encryption unit by providing the file in an encrypted manner) and wherein said network appliance further provides for the cipher processing of file data transferred in connection with said modified file request ([0204], lines 1-3, encryption key is provided for the cipher processing of file data transfer).

37. As to claim 15, Graham discloses wherein said policy data store further provides for the storage of an encryption key identifier determinable by said policy parser on evaluation of said file request message ([0093], lines 5-13) and wherein said network appliance obtains an encryption key identified by said encryption key identifier for use in the cipher processing of file data transferred in connection with said modified file request ([0204], Graham teaches of obtaining an encryption key identified in order to deliver the encryption key).

38. As to claim 16, Graham further discloses wherein said authentication data includes a process identifier ([0118], lines 1-2), corresponding to said application

program as executed on said client computer system ([0118], lines 8-12), a verified user identifier ([0160], lines 1-4), and a group identifier (page 13, table 1, lines 26-29), and wherein said policy parser is operative to qualify said file request message against said predetermined policy data with respect to said process identifier, verified user identifier, and group identifier ([0179], lines 1-3).

39. As to claim 17, Graham discloses a method of securing access by a client computer system to file data stored on a storage device accessible by said client computer system ([FIG. 1], said method comprising the steps of: a) intercepting, by a first program ([0064], lines 11-14, client module reads on first program) as executed on a client computer system (FIG. 1, item 150, [0140], client module filter driver, [0141], lines 1-3), a data transfer request issued by a second program, as executed on said client computer system ([0144], lines 9-13, the application reads on the second program), directed to a data file stored by a client accessible file data store ([0064], lines 1-5; and [0139], lines 12-15); b) first processing, by said first program, said data transfer request to associate authentication data with said data transfer request ([0128], lines 1-4); c) evaluating, by a security appliance coupled to said client computer system through a communications network (FIG. 1, proxy system 110, [0067], lines 1-10), said data transfer request, said authentication data, and access control data corresponding to said data file to qualify said data transfer request ([0101], lines 6-12, [0093], lines 5-13); and d) second processing to selectively enable said data transfer request to

proceed relative to said data file dependent on the qualification of said data transfer request ([0140], lines 8-14).

40. As to claim 18, Graham discloses the authentication data includes process ([0118], lines 1-2) and context identification information ([0175]).

41. As to claim 19, Graham discloses the authentication data includes a verified user identifier ([0160], lines 1-4) and a process identifier ([0118], lines 1-2).

42. As to claim 20, Graham further discloses the authentication data includes a verified user identifier ([0160], lines 1-4), a process identifier ([0118], lines 1-2), a group identifier (Table 1, lines 26-29).

43. As to claim 21, Graham discloses wherein said data transfer request specifies a data range of file data ([0141], lines 13, Graham inherently teaches of specifying a data range by making file requests to file servers) and wherein said second processing step includes the step of modifying said data range to accommodate block encryption of file data within said data file ([0141], lines 1-7).



Art Unit: 2196

44. As to claim 22, Graham discloses wherein said step of evaluating associates encryption control data with said data transfer request ([0141], lines 4-7) and wherein said second processing step, responsive to said encryption control data, includes cipher processing of file data transferred in connection with said data transfer request ([0141], lines 7-10, Graham teaches of including cipher processing by delivering the file in an encrypted format).

45. As to claim 23, Graham further discloses the steps of: a) first transferring said data transfer request to said security appliance through a first communications network ([0067], lines 1-10); and b) second transferring said data transfer request relative to said client accessible file data store through a second communications network ([0080], lines 9-14).

46. As to claim 24, Graham discloses that the security appliance is established a network portal through which network file accesses are routed between said client computer system and said client accessible file data store (FIG. 1, [0065], lines 9-14, Graham inherently teaches of establishing a network portal by providing the proxy system as a function of information which coupled with authentication system and policy system and with end-user client device through communication network in order to provide access to the network storage).

Art Unit: 2196

47. As to claim 25, Graham discloses a method of securing file access operations by a client computer system made with respect to a client accessible file data store (FIG. 1), said method comprising the steps of: a) intercepting, by a first program ([0064], lines 11-14, client module reads on first program) executing on a client computer system (FIG. 1, item 150, [0140], client module filter driver, [0141], lines 1-3), file operation requests issued by a second program, as executing on said client computer system ([0144], lines 9-13, the application reads on the second program), wherein said file operation requests are issued with respect to files stored in a filesystem accessible by said client computer system ([0064], lines 1-5; and [0139], lines 12-15); b) determining, by said first program relative to a predetermined file operation request, authentication data for said second program ([0128], lines 1-4), wherein said authentication data includes user and process identification data ([0160], lines 1-4, lines 6-8) and a representation of said predetermined file operation request ([0217]); and c) enabling, by a security appliance responsive to said authentication data (FIG. 1, proxy system 110, [0067], lines 1-10; and [0143], lines 1-2), said predetermined file operation request with respect to a file identified by said predetermined file operation request ([0175], lines 1-3), wherein said enabling step is dependent on qualification ([0101], lines 6-12, [0093], lines 5-13), by said security appliance (FIG. 1, proxy system 110), of said authentication data against policy data defining operation permissions relative to said file ([0101], lines 6-11; and [0140], lines 8-14).

Art Unit: 2196

48. As to claim 26, Graham further discloses a method of securing file access operations includes the steps of: a) associating an encryption key with said predetermined file operation request determined from the qualification of said authentication data against said policy data ([0093], lines 5-13, [0101], lines 6-12); and b) cipher processing, using said encryption key, file data transferred relative to said file ([0066], lines 7-11, cipher processing is done in order to provide the file in a secure and encryption manner).

49. As to claim 27, Graham discloses the step of cipher processing includes modifying the specification of said predetermined file operation request to accommodate encryption of file data transferred relative to said file ([0141], lines 1-7).

50. As to claim 28, Graham discloses the step of cipher processing is performed on said security appliance ([0092], lines 1-3; [0141], lines 7-10).

51. As to claim 29, Graham discloses authentication data includes a verified user identification ([0160], lines 1-4) and a login process identification ([0142], lines 4-12).

52. As to claim 30, Graham discloses a security appliance (FIG. 1; proxy system 110) for securing access by client computer systems to persistently stored data files (FIG. 1), said security appliance comprising: a) a processor coupleable to a client computer system to receive an access request message ([0064], lines 11-14, client module reads on processor), wherein said access request message includes authentication data ([0128], lines 1-4) and an identification of a file operation directed to an identified data file stored in a persistent data file store ([0217]); and b) a policy data store (FIG. 3, policy database 370, [0115], lines 1-4), accessible by said processor, providing for the storage of predetermined file operation qualifiers applicable to data files present in said persistent data file store ([0175], lines 1-3), wherein said policy data store is maintained secure by said processor with respect to said client computer system (FIG. 1, proxy system 110, [0107], lines 7-11), and wherein said processor is operative to selectively enable said file operation dependent on an evaluation of said predetermined file operation qualifiers with respect to said access request message ([0101], lines 6-12; and [0140], lines 8-14).

53. As to claim 31, Graham discloses the authentication data includes a verified user identifier ([0160], lines 1-4) and a group identifier (page 13, table 1, lines 26-29) and wherein said processor is operative to discriminate said verified user identifiers, said group identifier, said file operation and said identified data file against said predetermined file operation qualifiers to obtain said evaluation ([0101], lines 6-12).

54. As to claim 32, Graham discloses that the policy data store further provides for the storage of encryption keys in association with said predetermined file operation qualifiers ([0093], lines 5-13) and wherein said processor is operative to retrieve a predetermined encryption key from said policy data store dependent on said evaluation ([0204], Graham teaches retrieving an encryption key in order to deliver the encryption key).

55. As to claim 33, Graham discloses wherein said processor, responsive to said evaluation, is further operative to provide for said file operation to be passed to said persistent data file store ([0106], lines 3-8).

56. As to claim 34, Graham discloses wherein said processor, responsive to said evaluation, is further operative to modify a specification of said file operation to accommodate the transfer of encrypted data in connection with the performance of said file operation with respect to said identified data file ([0141], lines 1-4).

57. As to claim 35, Graham discloses wherein said processor includes an encryption engine operative to process encrypted data transferred with respect to said identified

data file ([0092], lines 1-3, Graham inherently teaches of using an encryption engine within the content subsystem).

### ***Conclusion***

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. See accompanying PTO 892.

Bata et. al. (Patent No.: US 6,901,403 B1) discloses the generation of a modified file request corresponding to a source file request.

Blumenau et al. (Patent No.: US 6,845,395) discloses for identifying a network path by which host processors are logged into the storage system.

Menninger et al. (Pub. No.: US 2003/0074355 A1) discloses a web portal application which supports distributed data warehouse that receives and stores data from different device over the public network.

Felsher (Pub. No.: US 2002/0010679 A1) discloses secure network storage infrastructure which provides encryption mechanism.

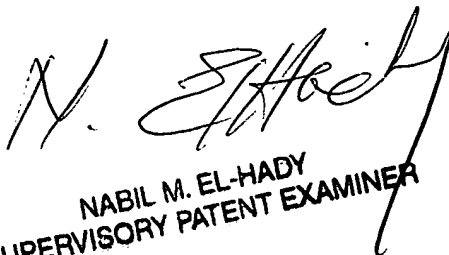
Any inquiry concerning this communication or earlier communications from the examiner should be directed to Suman Debnath whose telephone number is 571 270 1256. The examiner can normally be reached on 8 am to 5 pm.

Art Unit: 2196

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nabil M. El-Hady can be reached on 571 272-3963. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

SD  
SP  
11/09/06

  
NABIL M. EL-HADY  
SUPERVISORY PATENT EXAMINER